**Ověření úrovně kybernetické bezpečnosti dodavatelů a servisních středisek SOR**

Společnost, případně jeho organizační jednotka odpovědná za plnění dodávek pro SOR, provede vyplnění následujícího dotazníku definujícího úroveň jejího bezpečnostního standardu a z toho vyplývajících rizik kybernetické bezpečnosti. Tento dotazník slouží i jako kostra auditu při provádění případného ověření zákaznickým auditem SOR u dodavatele.

|  |  |
| --- | --- |
| **Dodavatel / ser. středisko (obchodní jméno, IČ):**  |  |
| Zodpovědná osoba za vyplnění (jméno, kontakt): |  |
| Datum vyplnění:  |  |
| **Vyhodnocení dotazníku**: (vyhovující, podmínečně vyhovující, nevyhovující) |  |
| **VYHODNOCENÍ DOTAZNÍKU*** **vyhovující** – plnění požadavků v úrovni C je méně než 25 %
* **podmínečně vyhovující s akčním plánem** – plnění požadavků v úrovni C je více než 25 % a méně než 75 %
* **nevyhovující** – požadavky v úrovni C o více než 75 %. Spolupráce s tímto dodavatelem je možná pouze ve výjimečných odůvodněných případech s nutným omezeným sdílení dat klasifikovaných stupněm důvěrné.
 |
| **ČESTNÉ PROHLÁŠENÍ**Výše zmíněná zodpovědná osoba, jako oprávněný zástupce dodavatele, čestně prohlašuje, že údaje v dotazníku níže odpovídají reálnému stavu ve společnosti dodavatele ke dni vyplnění dotazníku. Správnost těchto údajů je možné na vyžádání případně doložit zástupci SOR, případně ověřit provedením zákaznického auditu SOR u zákazníka, a to v době před uzavřením závazku nebo kdykoli v době jeho trvání.  V ………………….., dne …………………. kvalifikovaný elektronický podpis / vlastnoruční podpis oprávněné osoby. |
| **Oblast, požadavek** | **Dosažená úroveň (A, B, C)** | **Dosažená úroveň (A, B, C),****poznámka k plnění požadavku** |
| A | B | C |  |
| **A. STANDARDY** |
| 1 | Aplikuje dodavatel v praxi požadavky níže uvedeného standardu? |
| a. | Shoda s UN Regulation No. 155, 156 | Ano, certifikováno | Ano, necertifikováno | Ne |  |
| b. | ISO/IEC 27001 | Ano, certifikováno | Ano, necertifikováno | Ne |  |
| c. | ISO/SAE 21434 | Ano, certifikováno | Ano, necertifikováno | Ne |  |
| d. | TISAX | Ano, certifikováno | Ano, necertifikováno | Ne |  |
| e. | NIS2 | Ano, jsme zařazeni pod dohledem národního orgánu | Nejsme zařazeni, ale plníme všechny podmínky NIS2 | Ne |  |
| V případě, že bylo odpovězeno alespoň na jednu z předchozích otázek odpovědí ve sloupci A, prosíme o dodání certifikátu nebo jiného dokladu, není dále třeba pokračovat ve vyplňování dotazníku.Pokud nebyla dosažena úroveň A alespoň u jedné otázky, prosím pokračujte ve vyplňování následujícího dotazníku. |

|  |
| --- |
| **B. ZÁKLADNÍ OPATŘENÍ** |
| 2 | Má dodavatel manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností? | Ano, oddělená definovaná role | Ne, spadá pod IT, bez popisu role | Ne |  |
| 3 | Je u dodavatele prováděn audit či analýza, jejichž obsahem je kontrola v oblasti kybernetické bezpečnosti? | Ano, prováděna pravidelně | Ano, prováděna náhodně nebo nepravidelně | Ne |  |
| 4 | Provádí dodavatel hodnocení rizik v oblasti kybernetické bezpečnosti? | Ano, pravidelně, analýza rizik udržována | Ano, v minulosti provedena jednorázově | Ne |  |
| 5 | Které oblasti pokrývá řídící dokumentace (bezpečnostní politiky, směrnice využívání ICT, …) pokud taková dokumentace u dodavatele existuje? |
| a. | Procesy řízení rizik | Ano | Částečně řešeno | Neřešeno |  |
| b. | Klasifikace aktiv | Ano | Částečně řešeno | Neřešeno |  |
| c. | Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti | Ano | Částečně řešeno | Neřešeno |  |
| d. | Ochrana osobních dat | Ano | Jen rozsah dle GDPR | Neřešeno |  |
| e. | Identifikace a autentizace uživatelů | Ano | Částečně řešeno | Neřešeno |  |
| f. | Řízení přístupů k datům na základě práv | Ano | Částečně řešeno | Neřešeno |  |
| g. | Řízení privilegovaných přístupů | Ano | Částečně řešeno | Neřešeno |  |
| h. | Ochrana koncových stanic  | Ano | Částečně řešeno | Neřešeno |  |
| i. | Ochrana mobilních zařízení a vzdáleného přístupu | Ano | Částečně řešeno | Neřešeno |  |
| j. | Ochrana emailu a vnitrofiremní komunikace (instant messaging) | Ano | Částečně řešeno | Neřešeno |  |
| k. | Ochrana přístupu do internetu | Ano | Částečně řešeno | Neřešeno |  |
| l. | Ochrana výměnných médií | Ano | Částečně řešeno | Neřešeno |  |
| m. | Procesy řízení změn | Ano | Částečně řešeno | Neřešeno |  |
| n. | Ochrana bezdrátových sítí a komunikace | Ano | Částečně řešeno | Neřešeno |  |
| o. | Fyzická bezpečnost informačních aktiv | Ano | Částečně řešeno | Neřešeno |  |
| p. | Bezpečnostní školení koncových uživatelů a administrátorů | Ano | Částečně řešeno | Neřešeno |  |
| q. | Ochrana proti škodlivému softwaru | Ano | Částečně řešeno | Neřešeno |  |
| r. | Ochrana při výměně dat | Ano | Částečně řešeno | Neřešeno |  |
| s. | Procesy zvládání kybernetických incidentů | Ano | Částečně řešeno | Neřešeno |  |
| t. | Procesy řízení rizik dodavatelů | Ano | Částečně řešeno | Neřešeno |  |
| u. | Bezpečnost lidských zdrojů | Ano | Částečně řešeno | Neřešeno |  |
| v. | Bezpečnostní audity a analýzy | Ano | Částečně řešeno | Neřešeno |  |
| w. | Řízení kontinuity činností a havarijní plánování | Ano | Částečně řešeno | Neřešeno |  |
| **C. BEZPEČNOSTNÍ TECHNOLOGIE** |
| 6 | Které níže uvedené bezpečnostní technologie dodavatel provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům, vývoji SW nebo informačním systémům? |
| a. | Antivirový software na pracovních stanicích | Ano, komplexní řešení | Ano, základní řešení (Windows Defender) | Ne |  |
| b. | Antivirový software na mobilních zařízeních | Ano, součást komplexního řešení | Ano, dle každého uživatele | Ne |  |
| c. | Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System) | Ano | Ne | Ne |  |
| d. | Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management) | Ano | Ne | Ne |  |
| e. | Více-faktorová autentizace | Ano, využití mobilního zařízení nebo tokenu | Ano, bez využití mobilního zařízení nebo tokenu | Ne |  |
| f. | Automatizovaný nástroj pro řízení technologických zranitelností | Ano | Ne | Ne |  |
| g. | Nástroj pro řízení přístupu k síti (NAC, Network Access Control) | Ano | Ne | Ne |  |
| h. | Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service) | Ano, vč. napojení na SOC | Ano, ostrovně | Ne |  |
| i. | Šifrovací nástroje a techniky | Ano, použití přesně předepsáno | Ano, náhodně | Ne |  |
| j. | Firewall | Ano | Ano | Ne |  |
| k. | Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management) | Ano, včetně napojení na SOC | Ano, ostrovně | Ne |  |
| 7 | Byly interní systémy dodavatele někdy podrobeny penetračnímu testování? | Ano | Ne | Ne |  |
| **D. ŘEŠENÍ KYBERNETICKÝCH INCIDENTŮ** |
| 8 | Má dodavatel zaveden proces zvládání kybernetických incidentů? | Ano, vyhodnocovány systémově | Ano, vyhodnocovány ad-hoc nebo nesystémově | Ne |  |
| 9 | Jsou relevantní pracovníci dodavatele vzděláváni v oblasti rozpoznávání a reakce na kybernetické incidenty? | Ano, systematicky | Ano, ale nárazově | Ne |  |
| **E. ROZVOJ BEZPEČNOSTNÍHO POVĚDOMÍÍ** |
| 10 | Má dodavatel zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro pracovníky? | Ano, systémově řešeno | Nemá, jen nárazová školení | Ne, žádný rozvoj |  |
| 11 | Jsou noví zaměstnanci dodavatele vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? | Ano | Ano, nedostatečně | Ne |  |
| 12 | Dokumentuje dodavatel účast pracovníků na bezpečnostních školeních a vzdělávacích programech? | Ano | Ano | Ne |  |
| 13 | Vyžaduje dodavatel po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti? | Ano, u dat a IS, která toto vyžadují.  | Ne, nebo nekomplexně. | Ne |  |

|  |
| --- |
| **F. ZKUŠENOSTI DODAVATELE S KYBERNETICKÝMI INCIDENTY**Jaké negativní dopady pocítil dodavatel v souvislosti s kybernetickým incidentem, pokud v minulosti nastal: |
|  | **Dopad** | **Řešeno (ano/ne)** | **Bližší popis, jak bylo řešeno** |
| a. | Výpadek sítě |  |  |
| b. | Nedostupnost emailu a kancelářských aplikací |  |  |
| c. | Neoprávněné zneužití identity |  |  |
| d. | Prozrazení chráněných dat |  |  |
| e. | Ztráta nebo zničení dat |  |  |
| f. | Finanční ztráta |  |  |
| g. | Ztráta duševního vlastnictví |  |  |
| h. | Poškození pověsti organizace uchazeče |  |  |
| i. | Negativní publicita v médiích |  |  |
| j. | Ztráta hodnoty organizace uchazeče |  |  |
| k. | Trestní stíhání organizace uchazeče |  |  |